Dromore Road Primary School



Dromore Road is a small controlled Primary school situated in the town of Warrenpoint. We provide a broad and balanced education for children from

P1 – P7.

**E-SAFETY POLICY 2021**



# **Introduction**

# New technologies have become integral to the lives of children and young people in today’s society, both within school and in their lives outside of school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

# Currently the internet technologies children and young people could be using, both inside and outside of the classroom, include:

# Websites

# Learning Platforms and Virtual Learning Environments

# Email and Instant Messaging

# Chat Rooms and Social Networking

# Blogs and Wikis

# Podcasting

# Video Broadcasting

# Music Downloading

# Gaming

# Mobile/Smart phones with text, video and/or web functionality

# Other mobile devices with web functionality

# Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies. In Dromore Road Primary School we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

**Risks and Responses**

The Internet is an exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications’ channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable.

Key Concerns are:

**Potential Contact**

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, gaming, chat rooms or e-mail to communicate with children for inappropriate reasons. In our school children will be taught:

* That people are not always who they say they are.
* That “Stranger Danger” applies to the people they encounter through the Internet.
* That they should never give out personal details
* That they should never meet alone anyone contacted via the Internet
* That once they publish information (e.g. inappropriate photographs) it can be disseminated with ease and cannot be destroyed.

# Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content. Materials may express extreme views. e.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere. Materials may contain misleading and inaccurate information. e.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

In our school children will be taught:

* That information on the Internet is not always accurate or true.
* To question the source of information.
* How to respond to unsuitable materials or requests and that they should tell a teacher/ trusted adult immediately.

# Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children will be taught:

* Not to fill out forms with a lot of personal details.
* Not to use an adult’s credit card number to order online products.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

**Cyber Bullying**

We are very aware of the potential for pupils to be subjected to cyber bullying via e.g. texts, social – networking sites or emails. If it takes place within school, cyberbullying will be dealt with in line with the school’s overall anti-bullying policy, positive behaviour policy and pastoral services.

In our school children will be taught:

* If they feel they are being bullied by email, through social- networking sites, text or online they should always tell someone they trust.
* Not to reply to bullying, threatening text messages or emails as this could make things worse.
* Not to send or forward abusive texts or emails or images to anyone.
* Keep abusive messages as evidence.
* Not to photograph, film or record anyone without a teacher’s permission.

Children will be encouraged to report incidents of cyber-bullying to parents and the school to ensure appropriate action is taken.

Children will be encouraged to use websites such as [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) to learn how to deal with cyberbullying incidents which may take place outside of school. Should instances of online bullying and abuse be reported to the school by concerned parents, we will advise on how to report the incident to the appropriate authorities. Whilst, it is the parent’s ultimate responsibility for keeping their child safe at home, the school will also deal with incidences in line with our Anti-bullying policy, if appropriate,

We will keep records of cyber-bullying incidents, if they have occurred within school, to monitor the effectiveness of preventative activities, and to review and ensure consistency in investigations, support and sanctions.

**Roles and Responsibilities**

# As e-Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator (Mrs English) to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.

# The Principal/ICT Co-ordinator update the Governors with regard to e-safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

# **Writing and Reviewing the e-Safety Policy**

# This policy, supported by the school’s Acceptable Use Agreement is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Positive Behaviour, Child Protection, Pastoral Care and Anti-bullying.

# It has been agreed by the Staff and approved by the Board of Governors. The e-Safety policy and its implementation will be reviewed annually.

# **E-Safety Skills’ Development for Staff**

# All staff receive regular information and training on e-Safety issues through the co-ordinator at staff meetings or planned CPD sessions.

# All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

# New staff members receive information on the school’s Acceptable Use Agreement as part of their induction.

# All staff are encouraged to incorporate e-Safety activities and awareness within their lessons and by participating in annual Safer Internet Day.

# **E-Safety Information for Parents/Carers**

# Parents/ carers have an important role to play in promoting E-Safety. We encourage all parents/carers to become involved in e-Safety discussions with their child. The school website contains links to sites such as CEOP’s [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) which parents can use with their children. It is the responsibility of parents/ carers to be fully aware of what their child is doing online.

# The school communicates relevant e-safety information through parents’ sessions, information sheets and the school website.

# Parents/carers are asked to read through and sign the Acceptable Use Agreement with their child.

# Parents/ Carers are asked to make a decision as to whether they consent to images of their children being taken/ used in the school, including on our school website.

Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use. For example:

* Keep the computer in a communal area of the home.
* Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
* Monitor on-line time and be aware of excessive hours spent on the Internet.
* Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
* Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips (as listed on page 10).
* Discuss the fact that there are websites/social networking activities which are unsuitable and age restricted.
* Discuss how children should respond to unsuitable materials or requests.
* Remind children never to give out personal information online.
* Remind children that people on line may not be who they say they are.
* Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
* Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

**Teaching and Learning**

# **Internet use:**

# The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety.

# Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.

# Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.

# The school Internet access is filtered through the C2k managed service.

* No filtering service is 100% effective, therefore all children’s use of the Internet is supervised by an adult.
* Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

# Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

# Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

* The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
* Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
* Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

# **E-mail:**

* Children are not currently given individual e-mail addresses. In some instances, children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

# **Social Networking:**

* The school C2k system will block access to social networking sites.
* **Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.** However, we accept some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
* Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
* School staff will not add children as ‘friends’ if they use these sites.
* The school does not support and disapproves of the upload of incidental photographs of pupils taken at school events and would actively seek the support of parents / guardians in implementing this.

**Mobile Technologies:**

* The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
* Staff should not store pupils’ personal data and photographs on memory sticks.
* Pupils are not allowed to use personal mobile devices/phones in school.
* Staff should not use personal mobile phones during designated teaching sessions. The exception to this may be where devices are connected to speaker systems to play music e.g. during assembly.
* Pupils are not allowed to bring iPads, tablets, iPods, Dictaphones, smart watches or any other device that can photograph, film or record into school.

**iPads:**

iPads are used for digital storytelling, internet research and to support teaching and learning across the curriculum via the use of a range of appropriate apps. When using iPads, children will be reminded to be Internet wise and apply their Internet Safety rules. They will not be allowed to use iPads to:

* Take photographs of pupils/staff without permission or direction from the teacher.
* Take videos of pupils/staff without permission or direction from the teacher.

**Managing Video-conferencing:**

* Videoconferencing will be via the C2k network to ensure quality of service and security.
* Videoconferencing will be appropriately supervised.

**Publishing Pupil’s Images and Work**

* Parents/carers must give permission in writing if they wish images of their children to be taken and used on the school website, outside agencies or to be displayed in school. This permission is issued at the beginning of the school year and is considered valid for that school year unless there is a change in the child’s circumstances where consent could be an issue.
* Parents/carers may withdraw permission, in writing, at any time.
* Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
* Pupils’ full names will not be used anywhere on the School website
* Pupil’s work and photographs will only be published by outside agencies with the permission of the pupil and parents.

**Covid 19 Response**

Covid-19 has created a great deal of uncertainty in the lives of children and young people. Daily routines, family life, friendship groups and the safe space that schools provide have been disrupted. In the event of a return to remote learning the following arrangements as outlined in our Remote learning policy have been put in place to support families and monitor safety:

Where possible, all interactions will be textual and public.

All staff and pupils using video communication, e.g. a video lesson explanation or video evidence of learning must:

* Communicate in groups – one-to-one sessions are not permitted.
* Wear suitable clothing – this includes others in their household.
* Be situated in a suitable ‘public’ living area within the home with an appropriate background. ‘Private’ living areas within the home, such as bedrooms, are not permitted during video communication.
* Use appropriate language – this includes others in their household.
* Maintain the standard of behaviour expected in school.
* Use the necessary equipment and computer programs as intended.
* Not record, store, or distribute video material without permission.
* Always remain aware that they are visible.

All staff and pupils using audio communication must:

* Use appropriate language – this includes others in their household.
* Maintain the standard of behaviour expected in school.
* Use the necessary equipment and computer programs as intended.
* Not record, store, or distribute audio material without permission.
* Ensure they have a stable connection to avoid disruption to lessons.
* Always remain aware that they can be heard.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the Principal, in collaboration with the SENCO.

Pupils not using devices or software as intended will be disciplined in line with the Positive Behaviour Policy and or Anti-bullying Policy.

The school will inform parents prior to the period of remote learning about the methods of delivering remote teaching the school plans to use – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents via the school website about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

During the period of remote learning, the school will maintain regular contact with parents to:

* Reinforce the importance of children staying safe online.
* Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
* Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites
* Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

**Policy Decisions:**

# **Authorising Internet access**

# Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school’s e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms and in the school corridor.

# Access to the Internet will be supervised.

# All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school’s e-Safety rules and within the constraints detailed in the school’s e-Safety policy.

# All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

**Password Security:**

* Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared.
* All pupils are provided with an individual login username and password.
* Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
* Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

**Handling e-Safety Complaints:**

* Complaints of Internet misuse will be dealt with by the ICT co-ordinator and principal.
* Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the e-Safety incident logbook.
* Any complaint about staff misuse must be referred to the Principal.
* Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
* Pupils and parents will be informed of the complaints’ procedure.
* As part of the Acceptable use agreement children will know that if they deliberately break rules they could be stopped from using the internet and that parents/carers will be informed.

**Communicating the Policy:**

# **Introducing the e-Safety Policy to pupils**

* E-Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week, Internet safety day and whole school assemblies.
* Pupils will be informed that network and Internet use will be monitored**.**

**Staff and the e-Safety Policy:**

* All staff will be involved in discussions regarding E-Safety and will have access to a copy of the E Safety policy.
* Any information downloaded must be respectful of copyright, property rights and privacy.
* Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
* A laptop or iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

**Monitoring and review:**

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the Governors’ responsibility and they will review it’s effectiveness annually following consultation with the ICT co-ordinator and/or principal.

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_

(Chairperson)

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_

(Principal)

Co-ordinator \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_

(ICT Coordinator)

### Safety Rules for Children

#### Follow These SMART TIPS

**S**

**Secret -** Always keep your name, address, mobile phone number and password private – it’s like giving out the keys to your home!

**M**

**Meeting** someone you have contacted in cyberspace can be dangerous. Only do so with your parent’s/carer’s permission, and then when they can be present.

**A**

**Accepting** e-mails or opening files from people you don’t really know or trust can get you into trouble – they may contain viruses or nasty messages.

**R**

**Remember** someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

**T**

**Tell** your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Proctection Committees

### An Acceptable Use of the Internet

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

* On the network, I will only use my own login username and password.
* I will keep my username and password private.
* I will not access other people’s files without their permission.
* I will not change or delete other people’s work/files.
* I will ask permission before entering any website, unless my teacher has already approved that site.
* I will use the Internet for research and school purposes only.
* I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible.
* I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
* When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.
* I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
* If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
* I will not bring in memory sticks, mobile devices and recording devices (e.g. iPad, tablet, iPod, smart watches) to school unless I have been given permission by my teacher.
* I will never photograph, film or record anyone unless I have been given permission from my teacher.
* I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
* I will treat all ICT equipment with care
* I understand that if I deliberately break these rules I could be stopped from using the Internet/E-mail and my parents/carers will be informed.

**Our PRIMARY SCHOOL**

# Acceptable Use Agreement

# For Pupils

# Please complete and return this form to your child’s class teacher

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Pupil’s Name** |  | | **Class Teacher** | |  | |
| I have discussed and understood the e-safety agreement and will follow the rules which are there to keep me and the school safe. | | | | | | |
| **Pupil Name (print)** | |  | |  | | |
| **Pupil Signature** | |  | | **Date** | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Parent’s Name** |  | | | |
| As the parent or legal guardian of the pupil above, I have read and discussed the e-safety agreement with my child and give permission for my child to access the internet at school. I will encourage them to abide by these rules.  I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s e-safety.  I will ensure that any photographs taken during school events that include other children will not be shared using social media. | | | | |
| **Parents Name (print)** | |  |  | |
| **Parents Signature** | |  | **Date** |  |

### OUR PRIMARY SCHOOL

Acceptable Use Agreement

For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school’s Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

* All Internet activity should be appropriate to staff professional activity or the pupils’ education
* Access should only be made via the authorised account and password, which should not be made available to any other person
* Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
* Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
* Use for personal financial gain, gambling, political purposes or advertising is forbidden
* Copyright of materials must be respected
* Posting anonymous messages and forwarding chain letters is forbidden
* As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
* Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

|  |  |  |
| --- | --- | --- |
| **Name** |  | |
| **Date** |  | **Signed** |